AO 106 (Rev. 04/10) Application for a Search Warrant

UNDER SEAL

# UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia



In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

LG K20 PLUS, MODEL LGMP260, SERIAL NUMBER: S/N 708CYPY273016, CURRENTLY LOCATED AT 44965 AVIATION DRIVE, SUITE 112, DULLES, VA 20166

Case No. 1:18SW12

UNDER SEAL

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

THE LG K20 PLUS, MODEL LGMP260, SERIAL NUMBER: S/N 708CYPY273016 CURRENTLY LOCATED AT 44965 AVIATION DRIVE, SUITE 112, DULLES, VA 20166, as described in Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B (Items to be Seized)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 472 | Intent to defraud, bring into the United States, keep in his possession and conceal falsely made, forged, counterfeited, or altered obligations or other securities of the United States. |

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

DC Moore 1/8/18
*Applicant's signature*

Reviewed by AUSA/SAUSA:
Alexander Blanchard/Matthew Evans

Donald C. Moore, Special Agent, HSI
*Printed name and title*

Sworn to before me and signed in my presence.

/s/ JFA
John F. Anderson
United States Magistrate Judge
*Judge's signature*

Date: January 8, 2018

City and state: Alexandria, Virginia

Hon. John F. Anderson, U.S. Magistrate Judge
*Printed name and title*

**ATTACHMENT A**

1. The property to be searched consists of an LG K20 Plus smart type cellular phone, model LGMP260, bearing serial number 708CYPY273016 and International Mobile Equipment Identity ("IMEI") number 352130092730166 ("the Device"), which was found in the possession of Rulber DIAZ SALAZAR upon his international arrival at IAD, and which was detained by DHS/HSI via DHS Form 6051D. The Device is currently located at 44965 Aviation Drive, Suite 112, Dulles, Virginia 20166.

## ATTACHMENT B

1. All information and records on the Device described in Attachment A that constitutes evidence, fruits, contraband, and/or instrumentalities of violations of 18 U.S.C. § 472, including, but not limited to:

a. records regarding the identity and contact information of companies or individuals involved in the possession, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

b. records indicating travel purchased for, or otherwise obtained, and their related identifying and contact information for companies or individuals involved in the possession, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

c. records indicating companies or individuals involved in the possession, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

d. emails, text messages, exchanges over social media platforms, and/or other communications regarding the possession, creation, production, sale, provision, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

e. notes, photos, videos, or other electronically stored images or documents regarding the possession, creation, production, sale, provision, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

f. contact lists or phonebooks contained on the Device or in applications accessible on the Device;

g. call lists contained on the Device or in applications accessible on the Device;

h. all calendar entries contained on the Device or in applications accessible on the Device;

i. reminders contained on the Device or in applications accessible on the Device; and

j. a list of applications or software loaded onto the Device.

2. Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, phonebooks, photographs, videos, and correspondence.

3. Evidence of the presence or absence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

4. Evidence of the attachment of the Device to other storage devices, phones, or similar containers for electronic evidence.

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device.

6. Evidence of the times the Device was used.

7. Passwords, encryption keys, and other access devices that may be necessary to access the Device.

8. Documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device.

9. Records of, or information about, IP addresses used by this Device.

10. Records of, or information about, the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

11. All GPS information on the Device.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT IF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF THE LG K20 PLUS, MODEL LGMP260, SERIAL NUMBER: S/N 708CYPY273016 CURRENTLY LOCATED AT 44965 AVIATION DRIVE, SUITE 112, DULLES, VA 20166

Case No. 1:18SW12

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—namely, an electronic device—that is currently in law enforcement possession in Dulles, Virginia, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent Criminal Investigator with United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"). ICE/HSI is a subordinate component of the Department of Homeland Security ("DHS"). I have been a DHS/HSI Special Agent since June 2004, and I am currently assigned to the Washington Dulles International Airport ("IAD") Investigative Group at the HSI field office in Dulles, Virginia. In my capacity as an HSI Special Agent Criminal Investigator, I have had experience in criminal investigations involving counter proliferation, transnational gangs, commercial fraud, counterterrorism, immigration crimes, and financial crimes. I have been trained at the Federal Law Enforcement Training Center in Brunswick, Georgia, where I graduated from the Criminal Investigator Training Program, and the ICE Special Agent Training Program. In my capacity as

a Special Agent, my duties include investigating violations of the nation's immigration, nationality, and customs laws.

3. The facts and information contained in this affidavit are based upon my training and experience, participation in investigations, personal knowledge and observations during the course of this investigation, as well as the observations of other agents and officers involved in this investigation. All observations not personally made by me were relayed to me by individuals who made them or are based on my review of records, documents, and other physical evidence obtained during the course of this investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. For the reasons set forth in this affidavit, there is probable cause to believe that the item identified in Attachment A contain evidence, fruits, and/or instrumentalities of the importation into the United States, with intent to defraud, falsely made, forged, counterfeited, or altered obligations or other securities of the United States, in violation of 18 U.S.C. § 472.

## IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched consists of an LG K20 Plus smart type cellular phone, model LGMP260, bearing serial number 708CYPY273016 and International Mobile Equipment Identity ("IMEI") number 352130092730166 ("the Device"), which was found in the possession of Rulber DIAZ SALAZAR upon his international arrival at IAD, and which was detained by DHS/HSI via DHS Form 6051D. The Device is currently located at 44965 Aviation Drive, Suite 112, Dulles, Virginia 20166.

6. The applied-for warrant would authorize the forensic examination of the Device described in Exhibit A for the purpose of identifying electronically stored data particularly described in Attachment B.

**FACTUAL BASIS SUPPORTING PROBABLE CAUSE**

7. On December 14, 2017, DIAZ SALAZAR entered the United States at IAD in Dulles, Virginia, on Copa Airline flight CM 304, from Panama City, Panama, at approximately 1:45 pm. Upon entry, DIAZ SALAZAR had one carry-on bag and one checked bag that he retrieved from baggage claim. After DIAZ SALAZAR retrieved his checked bag from the baggage carousel, he was encountered by U.S. Customs and Border Protection ("CBP") officers. At the time of his arrival, DIAZ SALAZAR completed a Customs Declaration Form, CBP Form 6059B, in which he checked a box stating that he was not in possession of currency or monetary instruments over $10,000 in U.S. or foreign equivalent. DIAZ SALAZAR listed an address in Vienna, Virginia, as his destination.

8. Upon a secondary inspection conducted by CBP officers, DIAZ SALAZAR orally confirmed ownership of both his carry-on bag and his checked bag and orally stated he was in possession of $500. During a subsequent examination of his checked bag, CBP officers discovered, in the middle of a pair of tightly rolled pants, a bundle of $100 bills appearing to total $1,000 or more. When asked why he did not declare this money, DIAZ SALAZAR said that he did not remember that he had it. He was then asked if he had any more money in the bag, to which he responded that he did not. CBP officers continued their search of DIAZ SALAZAR's baggage and person, ultimately finding a total of $12,600 in counterfeit Federal Reserve Notes ("FRNs"), also known as U.S. currency, all in $100 denominations. The

counterfeit FRNs were separated into bundles of approximately $1,000 and secreted in numerous items of clothing within the checked bag.

9. Upon inspection of the FRNs, CBP observed that some of the notes had smeared ink and a texture that was inconsistent with genuine U.S. currency.

10. In addition to finding counterfeit FRNs, CBP also discovered seven fraudulent, unendorsed Western Union money orders, each bearing the same check number.

11. When asked why he did not declare the currency, DIAZ SALAZAR initially stated he did not remember that he had the bundle of currency in his checked bag. When asked why he concealed the currency in the checked bag, DIAZ SALAZAR stated he did not want the money to be found by authorities because he thought he was not permitted to carry over $5,000. DIAZ SALAZAR also stated he thought CBP would not find the money if hidden in multiple locations within his checked bag.

12. At approximately 4:35 pm, I initiated an interview of DIAZ SALAZAR. I introduced myself as a special agent with DHS/HSI. Spanish translation during the interview was provided by CBP Officer Santiago. I presented DIAZ SALAZAR with a Miranda Rights waiver in the Spanish language, which was also read to DIAZ SALAZAR in Spanish by CBP Officer Santiago. DIAZ SALAZAR stated that he understood his rights as stated, signed and dated the waiver, and agreed to speak to me. I asked DIAZ SALAZAR why he was visiting the United States, to which DIAZ SALAZAR responded he was visiting his brother, Juan Carlos Salazar, who resides in Vienna, Virginia.

13. I asked DIAZ SALAZAR to explain how he acquired the counterfeit currency. DIAZ SALAZAR stated he purchased the FRNs on the corner of 8th and 13th Streets in Bogota, Colombia. DIAZ SALAZAR stated that he purchased the FRNs on the street because he wanted

to get a better rate than offered in the legal currency exchange centers. DIAZ SALAZAR stated he saved approximately 1.5 million Colombian pesos (equivalent to approximately $500 U.S. dollars) by purchasing the FRNs on the street. DIAZ SALAZAR stated he suspected the currency might be counterfeit, but figured if it were counterfeit and he attempted to purchase items with it in the United States, merchants would simply refuse to accept the money. DIAZ SALAZAR stated the person who sold him the currency directed him to hide it in his checked baggage because "that kind of money" is not allowed in the United States.

14. I asked DIAZ SALAZAR where he obtained the Western Union money orders. DIAZ SALAZAR said that a man showed up at his house in Bogota and asked DIAZ SALAZAR to deliver the money orders to Juan Carlos Salazar in the United States. According to DIAZ SALAZAR, the unknown man directed him to take the money orders to Juan Carlos Salazar's store where someone else would pick them up. DIAZ SALAZAR stated he did not know the man who came to his house, but that the man knew DIAZ SALAZAR's name, address, and brother, Juan Carlos Salazar.

15. During further inspection of DIAZ SALAZAR's belongings, a business credit card in DIAZ SALAZAR's name was discovered. This business credit card listed the business name "DC PRODUCTION." DIAZ SALAZAR stated that card was for his brother's business. I asked DIAZ SALAZAR if he was partners with his brother in the United States. DIAZ SALAZAR stated he was, but that he had recently given the company to Juan Carlos Salazar.

16. During the interview, DIAZ SALAZAR requested to access the Device in order to retrieve the home address and telephone number of his brother, Juan Carlos Salazar.

17. In addition to the business credit card, I also discovered an extra T-Mobile Subscriber Identity Module ("SIM") card, bearing number 8901260755759885390, taped to a

business card for "IPHONES DC," which DIAZ SALAZAR had stated was Juan Carlos Salazar's business and where he was instructed to deliver the fraudulent money orders.

18. On December 27, 2017, the United States Secret Service ("USSS") analyzed the $100 FRNs, concluding that all 126 of them are counterfeit. USSS further concluded that one of the FRNs is a new circular, indicating that it was manufactured with a printing plate not previously encountered by USSS.

19. In previous experience, I have seen that cell phones, such as the Device described in Exhibit A, are often instruments used to carry out and/or facilitate the importation and distribution of prohibited items into and throughout the United States. Accordingly, I submit that there is probable cause to believe that DIAZ SALAZAR utilized the Device described in Attachment A in communicating with Juan Carlos Salazar and/or the supplier of the counterfeit FRNs and fraudulent money orders. I further submit that there is probable cause to believe that the Device contains evidence of, and is itself an instrumentality of, DIAZ SALAZAR's violation of 18 U.S.C. § 472.

20. Based on my training and experience, I know that co-conspirators, in furtherance of their conspiracy to bring prohibited items into the United States, frequently use cell phones, such as the Device described in Exhibit A, to communicate with one another. Such communications may take the form of text messages, emails, and/or other forms of electronic communication which, based on my training and experience, I know can remain on cell phones and SIM cards for years.

21. Based on my training and experience, I also know that conspirators often retain pictures on their cell phones that link them to their co-conspirators and document acts in

furtherance of the conspiracy to carry out and/or facilitate the importation and distribution of prohibited items into and throughout the United States.

22. Based on my training and experience, I also know that cell phones often contain information, including GPS information, revealing the devices' geographic locations at points in time.

23. The Device is currently in the lawful possession of the DHS/HSI. It came into the DHS/HSI's possession during the secondary customs inspection of DIAZ SALAZAR as an international arriving passenger from Colombia on December 14, 2017.

24. The Device, having been in the continuous possession of law enforcement since it was initially seized, is currently in storage at 44965 Aviation Drive, Suite 112, Dulles, Virginia 20166. It, and its contents, remain in substantially the same state it was when it first came into the possession of the DHS/HSI.

## TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, cellular telephone, or cell phone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include:

storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts

of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer

software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. SIM Card: A SIM card is a small card that contains a cellular network subscriber's account information, which allows the device to authenticate to the network to which it is connected. SIM cards may store limited amounts of recoverable data such as telephone numbers, text messages, location information to include last connected tower, phone book, and subscriber information. Moving

a SIM card from one phone to another allows a subscriber to switch cell phones without having to contact their network carrier.

i. IMEI Number: The International Mobile Equipment Identity ("IMEI") is a unique number given to every single cellular device.

26. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://www.t-mobile.com, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device along with evidence tied to importing prohibited items via phone contacts with co-conspirators, text messages with co-conspirators, photos of co-conspirators and locations where the exchange of prohibited items is occurring, GPS coordinates detailing where various co-conspirators are located, and IP logs indicating where the user of the phone was located when accessing the internet.

## ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crime described in the warrant, but also forensic evidence that establishes how

the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the electronic device was used, the purpose of its use, who used it, and when it was used.

d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a cell phone is evidence may depend on other information stored on the cell phone and the application of knowledge about how a cell phone behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is, or whether it contains, evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

31. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seize the items described in Attachment B.

## REQUEST FOR SEALING

32. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation that is neither public nor known to all of the targets of the investigation. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this

affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

DC Moore 1/8/18

Donald C. Moore
Special Agent
Homeland Security Investigations
U.S. Department of Homeland Security

Subscribed and sworn to before me
on January 8, 2018:

/s/ JFA
John F. Anderson
United States Magistrate Judge

Hon. John F. Anderson
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

1. The property to be searched consists of an LG K20 Plus smart type cellular phone, model LGMP260, bearing serial number 708CYPY273016 and International Mobile Equipment Identity ("IMEI") number 352130092730166 ("the Device"), which was found in the possession of Rulber DIAZ SALAZAR upon his international arrival at IAD, and which was detained by DHS/HSI via DHS Form 6051D. The Device is currently located at 44965 Aviation Drive, Suite 112, Dulles, Virginia 20166.

**ATTACHMENT B**

1. All information and records on the Device described in Attachment A that constitutes evidence, fruits, contraband, and/or instrumentalities of violations of 18 U.S.C. § 472, including, but not limited to:

a. records regarding the identity and contact information of companies or individuals involved in the possession, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

b. records indicating travel purchased for, or otherwise obtained, and their related identifying and contact information for companies or individuals involved in the possession, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

c. records indicating companies or individuals involved in the possession, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

d. emails, text messages, exchanges over social media platforms, and/or other communications regarding the possession, creation, production, sale, provision, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

e. notes, photos, videos, or other electronically stored images or documents regarding the possession, creation, production, sale, provision, production, receipt, acquisition, transportation, concealment, and/or distribution of falsely made, forged, counterfeited, or altered obligations or other securities of the United States and/or fraudulent money orders;

f. contact lists or phonebooks contained on the Device or in applications accessible on the Device;

g. call lists contained on the Device or in applications accessible on the Device;

h. all calendar entries contained on the Device or in applications accessible on the Device;

i. reminders contained on the Device or in applications accessible on the Device; and

j. a list of applications or software loaded onto the Device.

2. Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, phonebooks, photographs, videos, and correspondence.

3. Evidence of the presence or absence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

4. Evidence of the attachment of the Device to other storage devices, phones, or similar containers for electronic evidence.

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device.

6. Evidence of the times the Device was used.

7. Passwords, encryption keys, and other access devices that may be necessary to access the Device.

8. Documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device.

9. Records of, or information about, IP addresses used by this Device.

10. Records of, or information about, the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

11. All GPS information on the Device.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.